Serial No. 09/681,804
Art Unit: 2131

AMENDMENTS TO THE CLAIMS

Please amend the claims as indicated hereafter. The present claim listing replaces all prior versions of the claims.

Claims:

1-28 (Canceled).

29. (Currently amended)   A method for authorizing execution of an object on a computer system comprising:

    (a)   selecting an executable object on the computer system;

    (b)   inserting a first identifier into a steganographic zone of the object, wherein the first identifier and the stenographic zone of the object are formed by the computer system and the first identifier prevents execution of the executable object; and

    (c)   comparing the first identifier in the steganographic zone to a second identifier each time the object is selected for execution, wherein an executable version of the object is created by extracting the first identifier from the executable object if the first identifier matches the second identifier.

30. (Previously presented)   The method of claim 29, wherein the identifiers comprise a sequence of fields for creating a unique copy of the object and an ownership token between the object and the system.

31. (Previously presented)   The method of claim 29, wherein the second identifier is stored on the system.

32. (Previously presented)   The method of claim 29, wherein the second identifier is stored on an external data storage structure.

3

33. (Canceled)

34. (Previously presented) The method of claim 32, wherein the external data storage device comprises data for extracting the first identifier.

35. (Previously presented) The method of claim 29, wherein the second identifier is encrypted.

36. (Currently amended) A method for identifying unauthorized objects on a computer system comprising:

(a) authorizing objects of the computer system by embedding a system identifier into the authorized objects;

(b) determining the presence of the system identifier in objects of the computer, wherein objects that are not embedded with the system identifier are unauthorized; ~~and~~

(c) isolating unauthorized objects from the computer system; <u>and</u>

(d) <u>creating an executable version of authorized objects by extracting the system identifier each time a request for execution of the authorized objects is received.</u>

37. (Previously presented) The method of claim 36, wherein the identifiers comprise a sequence of fields for creating a unique copy of the object and an ownership token between the object and the system.

38. (Previously presented) The method of claim 36, wherein the system identifier is stored on the system.

39. (Previously presented) The method of claim 36, wherein the system identifier is stored on an external data storage structure.

4

40. (Previously presented)   The method of claim 36, wherein the system identifier is embedded in a steganographic zone of the authorized object.

41. (Currently amended)   The method of claim [[36]] 40, wherein the system identifier is extracted from the steganographic zone of the object.

42. (Previously presented)   The method of claim 39, wherein the external data storage device comprises data for extracting the system identifier.

43. (Previously presented)   The method of claim 36, wherein the system identifier is encrypted.

44. (Currently amended)   A method for authorizing objects of a computer system comprising:

   (a)   selecting a set of objects for authorization;

   (b)   generating a system identifier, wherein the system identifier is generated by the computer system using object fields;

   (c)   embedding the selected objects with the system identifier, wherein objects with an embedded system identifier are not executable;

   (d)   storing the system identifier;

   (e)   determining the presence of the system identifier on objects on the computer system;

   (f)   comparing detected system identifiers on the objects of the computer system with the stored system identifier; and

   (g)   isolating objects without a detectable system identifier or with a system identifier that does not match the stored system identifier; and

5

(h)   creating an executable version of authorized objects by extracting the system identifier each time a request for execution of the authorized objects is received.

45.   (Previously presented)   The method of claim 44, wherein the system identifier comprises a sequence of fields for creating a unique copy of the object and an ownership token between the object and the system.

46.   (Previously presented)   The method of claim 44, wherein the system identifier is stored on the system.

47.   (Previously presented)   The method of claim 44, wherein the system identifier is stored on an external data storage structure.

48.   (Previously presented)   The method of claim 44, wherein the system identifier is embedded in a steganographic zone of the object.

49.   (Previously presented)   The method of claim 48, wherein the system identifier is extracted from the steganographic zone of the object.

50.   (Previously presented)   The method of claim 47, wherein the external data storage device comprises data for extracting the first identifier.

51.   (Previously presented)   The method of claim 44, wherein the stored system identifier is encrypted.

52.   (Currently amended)   A method for creation of authorized objects of a computer system comprising:

        (a)   selecting an executable object for authorization;

        (b)   retrieving a system identifier from a storage device;

6

(c)   embedding the selected object with the system identifier wherein the system identifier prevents execution of the object;

(d)   storing data for retrieving the system identifier from the object on the storage device and generating an executable copy of the object each time the object is selected for execution <u>by extracting the system identifier from the object</u> if the first identify matches the second identifier.

53.   (Previously presented) The method of claim 52, wherein the system identifier comprises a sequence of fields for creating a unique copy of the object and an ownership token between the object and the system.

54.   (Previously presented)   The method of claim 52, wherein the system identifier is retrieved from an external data storage structure.

55.   (Previously presented)   The method of claim 52, wherein the system identifier is embedded in a steganographic zone of the object.

56.   (Previously presented)   The method of claim 54, wherein the external data storage device comprises data for extracting the first identifier.

57.   (Previously presented)   The method of claim 52, wherein the stored system identifier is encrypted.

7